From:	Lemons Terry L
To:	Lipold John A; Brace Taylor; Allen Sarah; Andrews Sheila L; angela_camp@intuit.com; Ashley McMahon; Asper Damon C; Azalea DeFord; Bernie McKay; Bond, Shannon (Shannon.Bond@wolterskluwer.com); Brennan Lynn M; Burch Stephanie C; Burkhart Brent L; Christopher Russell; Connelly Karen A; Courtney Decker; Cresson Frederick L; Crews Craig E; Daniel Eubanks; Dave Ransom; Eguren Sara L; Eldridge Michelle L; Emily Landis; Erica Koslowsky; Erik Inkrott; Ferguson Shane; Hardy Mel; Hull, Vickie (Vickie.Hull@timhugo.com); James Carson; James Gazzale; JC Craig; "Joe.Sica@sbtpg.com"; John Ams; Johnston Alec S; Jonathan Lyon; Julia Fletcher; Kerns Chris D; Kpickering@hrblock.com; Laura Fallon; Leann Boswell; Luanne Brown; lynne.riley@dor.ga.gov; Mark Castro; Maser Peter E; Mathis Nancy; Mealy Filomena; Melissa Netram; Mercado Wayne R; Michael Blache; Michael Fulmer; Michelle Cain; Migazzi Donna J; Nadal Yadira G; Pachner Anny K; Pryde Joan A; Ramsey Maryclaire; Reynolds Jodie M; Romaniello Margaret A; Sharonne Bonardi; Sincox Terri; Stepter Deirdre H; Steve Ryan; Susan Waldron; Tim Hugo@capnet.org (Tim.Hugo@capnet.org); Smith Verenda; doreen.warren.id@gmail.com
Cc:	Polnak, Penni A (TAX); Mark Castro; Beebe Michael C; Deneroff Michael; Campbell Carol A; gene.salo@thomsonreuters.com; James Sharon C; Sambandam, Raja, TRD; Robert_Pivoris@intuit.com; Davis Denise D; Powell Tamara S; Rossi-Franzke Theresa; terry.garber@taxadmin.org; Jami Gibson; Stetler Sharon D; Singletary Lamar; nancy.guglielmo@fsroundtable.org; Salas Santos Lizette; Landreth Kristen A; Killen Edward T; Grimes Phyllis T; Oser Michael J; D"Ambrosio John; CERCA; John.Sapp@drakesoftware.com; Clemens, Tammy; Melissa.Smith@illinois.gov; Goins Catherine H; Horn Carl W II; Conner Akeia P; Emblom Ed F; "btate@nbpca.org"; Giardina Clare L [Contractor]; Robinson Sadiqa T; McKnight Abigail K; Shaw Jamie L; Nancy Guglielmo
Subject:	DRAFT COPIES: Tax Security Awareness Week news releases
Date:	Wednesday, November 21, 2018 11:47:00 AM
Attachments:	IR-2018 NTSAW 1 online shoppingA.docx IR-2018 NTSAW 2 phishingA.docx IR-2018 NTSAW 3 new password guidance (002).docx IR-2018 NTSAW 4 IDT W2 scamsA.docx IR-2018 NTSAW 5 Tax pros data theft.docx

---

Summit Communications Team members – sharing draft versions of the news releases for Tax Security Awareness Week. Copies are attached. As you will see, these drafts still have some spots to plug in. The topics cover:

Monday, Dec. 3 – Online shopping
Tuesday, Dec. 4 - phishing
Wednesday, Dec. 5 – updated password guidelines
Thursday, Dec. 6 – W-2 scams
Friday, Dec. 7 – Tax professional data theft

Please let us know if any comments or feedback on these – including whether we need any additional details for states or industry – by COB Monday if possible so we can quickly finalize these.

Additional updates:
*We plan to set up a Summit Communications team call mid-day on Tuesday to touch on any remaining topics for Tax Security Awareness Week. John Lipold will be sending out an invite.
*We are now over 30 different press and partner events. We will share an updated list on Monday; if you have interest in participating in a specific event, please let John and me know. (Short list of current locations below).
*If your group has interest in including a supporting press statement to the materials, please let us know. We'll include any supporting statements in the Monday kick-off package.

Thanks, and happy Thanksgiving!
Terry

City	State
Denver	CO
Chicago	IL
Cranston	RI
San Diego	CA
Union City	CA
Southfield	MI
Dallas	TX
Miami	FL
Texarkana	AR
Milwaukee	WI
Kansas City	KS
Detroit	MI
Los Angeles	CA
Houston	TX
Kenner	LA
Hartford	CT
Philadelphia	PA

TBD	WV
Atlanta	GA
Mission Viejo	CA
Harligen	TX
Citrus Heights	CA
Cleveland	OH
Richmond	VA
Portland	ME
Lawrence	MA
Dallas	TX
New York	NY
Hollywood	CA
St. Louis	MO

News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

12 | 03 | 18 – DRAFT DRAFT DRAFT DRAFT

IRS, Security Summit Partners warn public:
It's shopping season for identity thieves, too; Tax Security Awareness Week offers tips

IR-2018-xxx

WASHINGTON — With the holiday shopping season in full swing, the Internal Revenue Service and Security Summit partners warn taxpayers to take extra steps to protect their tax and financial data from identity thieves.

The holidays offer cybercriminals a chance to steal financial account information, Social Security numbers, credit card information and other sensitive data to help them file a fraudulent tax return in 2019.

The Internal Revenue Service, state tax agencies and the tax community, partners in the Security Summit, are marking "National Tax Security Awareness Week" Dec. 3 -7, with a series of reminders to taxpayers and tax professionals. In part one, the topic is online shopping.

(IRS quote)

In part one of a weeklong series of tips, the Summit partners warn people shopping online or in public places to remember a few basic tips that can go a long way to protecting their identity and personal information. This is part of the Summit's "Taxes.Security.Together." campaign.

Cybercriminals seek to turn stolen data into quick cash, either by draining financial accounts, charging credit cards, creating new credit accounts or even using stolen identities to file a fraudulent tax return for a refund.

Here are seven steps to help with online safety and protecting tax returns and refunds:

- *Avoid unprotected Wi-Fi.* Unprotected public Wi-Fi hotspots in malls or at holiday events also may allow thieves to view transactions. Do not engage in online financial transactions if using unprotected public Wi-Fi.
- *Shop at familiar online retailers.* Generally, sites using the "s" designation in "https" at the start of the URL are secure. Look for the "lock" icon in the browser's URL bar. But remember, even bad actors may obtain a security certificate so the "s" may not vouch for the site's legitimacy. Beware of purchases at unfamiliar sites or clicks on links from pop-up ads.
- *Learn to recognize and avoid phishing emails that pose as a trusted source such as those from financial institutions or the IRS.* The IRS has seen an increase in these schemes this year. These emails may suggest a password is expiring or an account update is needed. The criminal's goal is to entice users to open a link or attachment. The link may take users to a fake website that will steal usernames and passwords. An attachment may download malware that tracks keystrokes -- putting personal information at risk.
- *Keep a clean machine.* This applies to all devices – computers, phones and tablets. Use security software to protect against malware that may steal data and viruses that may damage files. Set it to update automatically so that it always has the latest security defenses. Make sure firewalls and browser defenses are always active. Avoid "free" security scans or pop-up advertisements for security software.

- *Use passwords that are strong, long and unique.* Experts suggest a minimum of 10 characters but longer is better. Avoid using a specific word; longer phrases are better. Use a combination of letters, numbers and special characters. Use a different password for each account. Use a password manager, if necessary.
- *Use multi-factor authentication.* Some financial institutions, email providers and social media sites allow users to set accounts for multi-factor authentication. This means users may need a security code, usually sent as a text to a mobile phone, in addition to usernames and passwords.
- *Encrypt and password-protect sensitive data.* If keeping financial records, tax returns or any personally identifiable information on computers, this data should be encrypted and protected by a strong password. Also, back-up important data to an external source such as an external hard drive. And, when disposing of computers, mobile phones or tablets, make sure to wipe the hard drive of all information before trashing.

The IRS, state tax agencies and the tax industry are committed to working together to fight against tax-related identity theft and to protect taxpayers. But the Security Summit needs help. With the steps listed above, people can take steps to protect themselves online.

Taxpayers can also visit the "Taxes. Security. Together." awareness campaign or review Publication 4524, Security Awareness for Taxpayers, to see what can be done.Tax professionals can also get more information through the Protect Your Clients; Protect Yourself campaign as well as the Tax Security 101 series.

-30-

News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

12 | 04 | 18 DRAFT DRAFT DRAFT DRAFT

IRS sees surge in email phishing scams; Summit Partners urge taxpayers: 'Don't Take the Bait'

IR-2018-xxx

WASHINGTON — With the approach of the holidays and the 2019 filing season, the Internal Revenue Service, state tax agencies and the nation's tax industry warned people to be on the lookout following a surge of new, sophisticated email phishing scams.

Taxpayers saw many more phishing scams in 2018 as the IRS recorded a xx percent increase in bogus email schemes that seek to steal money or tax data. These schemes can endanger a taxpayer's financial and tax data, allowing identity thieves a chance to try stealing a tax refund.

The Internal Revenue Service, state tax agencies and the tax community, partners in the Security Summit, are marking "National Tax Security Awareness Week" Dec. 3 -7, with a series of reminders to taxpayers and tax professionals. In part two, the topic is email phishing scams.

IRS quote

In the second part of this week's National Tax Security Awareness Week series, the IRS and Summit partners warned against a new influx of phishing scams.

Tax-related phishing scams reported to the IRS declined for the prior three years until a surge in 2018. *Updated statistics*

One recent malware campaign used a variety of subjects like "IRS Important Notice," "IRS Taxpayer Notice" and other variations. The phishing emails, which use varying language, demands a payment or threatens to seize the recipient's tax refund.

Taxpayers can help spot these schemes by examples of misspelling and bad grammar. Taxpayers can forward these email schemes to phishing@irs.gov.

The most common way for cybercriminals to steal money, bank account information, passwords, credit cards or Social Security numbers is to simply ask for them. Every day, people fall victim to phishing scams or phone scams that cost them their time and their cash.

Phishing attacks use email or malicious websites to solicit personal, tax or financial information by posing as a trustworthy organization. Often, recipients are fooled into believing the phishing communication is from someone they trust. A scam artist may take advantage of knowledge gained from online research and earlier attempts to masquerade as a legitimate source, including presenting the look and feel of authentic communications, such as using an official logo. These targeted messages can trick even the most cautious person into taking action that may compromise sensitive data.

The scams may contain emails with hyperlinks that take users to a fake site. Other versions contain PDF attachments that may download malware or viruses.

Some phishing emails will appear to come from a business colleague, friend or relative. These emails might be an email account compromise. Remember, criminals may have compromised your friend's email account and begin using their email contacts to send phishing emails.

Not all phishing attempts are emails – some are phone scams. One of the most common phone scams is the caller pretending to be from the IRS and threatening the taxpayer with a lawsuit or with arrest if payment is not made immediately, usually through a debit card.

In addition, phishing@irs.gov continues to receive a large volume of IRS telephone scam complaints. These phone scams increased again in 2018 with reports to phishing@irs.gov recording thousands of telephone numbers from email complaints each week.

Phishing attacks, especially online phishing scams, are popular with criminals because there is no fool-proof technology to defend against them. Users are the main defense. When users see a phishing scam, they should ensure they don't take the bait.

Here are a few steps to take to protect against phishing and other tax-related schemes:

- *Be vigilant; be skeptical*. Never open a link or attachment from an unknown or suspicious source. Even if the email is from a known source, approach with caution. Cybercrooks are adept at mimicking trusted businesses, friends and family -- including the IRS and others in the tax business. Thieves may have compromised a friend's email address, or they may be spoofing the address with a slight change in text, such as name@example.com vs narne@example.com. In the latter, merely changing the "m" to an "r" and "n" can trick people.
- *Remember, the IRS doesn't initiate spontaneous contact with taxpayers by email to request personal or financial information*. This includes asking for information via text messages and social media channels. The IRS does not call taxpayers with aggressive threats of lawsuits or arrests.
- *Phishing schemes thrive on people opening the message and clicking on hyperlinks*. When in doubt, don't use hyperlinks and go directly to the source's main web page. Remember, no legitimate business or organization will ask for sensitive financial information via email.
- *Use security software to protect against malware and viruses found in phishing emails.* Some security software can help identity suspicious websites that are used by cybercriminals.
- *Use strong passwords to protect online accounts.* Each account should have a unique password. Use a password manager if necessary. Criminals count on people using the same password repeatedly, giving crooks access to multiple accounts if they steal a password - creating opportunities to build phishing schemes. Experts recommend the use of a passphrase, instead of a password, use a minimum of 10 digits, including letters, numbers and special characters. Longer is better.
- *Use multi-factor authentication when offered*. Some online financial institutions, email providers and social media sites offer multi-factor protection for customers. Two-factor authentication means that in addition to entering your username and password, you must enter a security code generally sent as a text to your mobile phone. Even if a thief manages to steal usernames and passwords, it's unlikely the crook would also have a victim's phone.

The IRS, state tax agencies and the tax industry are working together to fight against tax-related identity theft and to protect taxpayers. Everyone can help. Visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers, to learn more. Tax professionals can also get more information through the Protect Your Clients; Protect Yourself campaign as well as the Tax Security 101 series.

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

12 | 05 | 18 DRAFT DRAFT DRAFT DRAFT

Security Summit Partners highlight new password guidance, urge taxpayers and practitioners to protect all accounts

IR-2018-XXX

WASHINGTON – To help protect against cybercriminals stealing identities, the IRS, state tax agencies and the nation's tax industry urged people to review new, stronger standards to protect the passwords of their online accounts.

Every individual or tax practitioner who maintains any type of online accounts should use strong passwords to protect against savvy cybercriminals taking over their identities and accessing sensitive tax and financial data.

But there's been some new thinking as to what a strong password is. The latest guidance suggests using a passphrase such as a favorite line from a movie or a series of associated words rather than using a password. The idea is to create a passphrase that can be remembered easily and protect the account. This means passwords like – "uE*s3P%8V)" – are out. Longer, personal phrases people can remember – for example, SunWalkRainDrive – are now preferred.

The Internal Revenue Service, state tax agencies and the tax community, partners in the Security Summit, are marking "National Tax Security Awareness Week," Dec. 3-7, with a series of reminders to taxpayers and tax professionals. In part three, the topic is creating a strong password.

This is especially important for taxpayers and tax professionals who use online accounts involving financial data or even their online account with the IRS or a tax software provider.

IRS quote

The IRS, like all federal agencies, follows the cybersecurity framework set by the National Institute of Standards and Technology or NIST, which is a branch of the Department of Commerce. NIST last year rethought its guidance on passwords.

NIST suggested these three steps to build a better password:

- Step 1 – Leverage your powers of association. Identify associated items that have meaning to you.
- Step 2 – Make the associations unique to you. Passphrases should be words that can go together in your head, but no one else would ever suspect. Good example: Items in your living room such as BlueCouchFlowerBamboo. Bad example: Names of your children.
- Step 3 – Picture this. Create a passphrase that you can picture in your head. In our example, picture items in your living room. The key is to create a passphrase that is hard for a cybercriminal to guess but easy for you to remember.

In additional to creating strong passwords, the Security Summit urges taxpayers and tax practitioners to take these additional steps:

- Use a different password or passphrase for each account; use a password manager if necessary for multiple accounts.
- Use multi-factor authentication whenever possible. Don't rely on the passphrase alone to protect sensitive data. Multi-factor authentication means returning account holders need more than just their credentials (username and password) to access an account. They also need, for example, a security code sent as text to a mobile phone. Email providers and social media outlets, such as Facebook, offer multi-factor authentication options. For tax professionals, some tax software providers will offer multi-factor authentication as an option, and practitioners should use it if it's available.
- Change all factory-set passwords for wireless devices such as printers and routers. Again, use strong passphrases to protect access to these devices, which further safeguards sensitive data.

The IRS, state tax agencies and the tax industry are committed to working together to fight against tax-related identity theft and to protect taxpayers. But the Security Summit needs help. People can take steps to protect themselves online.

Taxpayers can visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers, for additional steps to protect themselves and their data from identity theft. Tax professionals can get more information through the Protect Your Clients; Protect Yourself campaign as well as the Tax Security 101 series.

-30-

IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

12 | 06 | 18 DRAFT DRAFT DRAFT DRAFT

Security Summit warns employers: Be alert to identity theft and W-2 scams

IR-2018-XXX

WASHINGTON – As the 2019 tax season approaches, the IRS, state tax agencies and the nation's tax industry joined together to warn small businesses to be on-guard against a growing wave of identity theft and W-2 scams.

Small business identity theft is a big business for identity thieves. Just like individuals, businesses may have their identities stolen and their sensitive information used to open credit card accounts or used to file fraudulent tax refunds for bogus refunds. Employers also hold sensitive tax data on employees, such as Form W-2 data, which also is highly valued by identity thieves.

The Internal Revenue Service, state tax agencies and the tax community, partners in the Security Summit, are marking "National Tax Security Awareness Week," Dec. 3-7, with a series of reminders to taxpayers and tax professionals. In part four, the topic is business-related identity theft and scams.

Identity thieves have long made use of stolen Employer Identification Numbers (EINs) to create fake Forms W-2 that they would file with fraudulent individual tax returns. Fraudsters also used EINs to open new lines of credit or obtain credit cards. Now, they are using company names and EINs to file fraudulent returns.

The IRS has identified an increase in the number of fraudulent Forms 1120, 1120S and 1041 as well as Schedule K-1. The fraudulent filings apply to partnerships as well as estate and trust forms.

Business, partnerships and estate and trust filers should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- Extension to file requests are rejected because a return with the Employer Identification Number or Social Security number is already on file;
- An e-filed return is rejected because of a duplicate EIN/SSN is already on file with the IRS;
- An unexpected receipt of a tax transcript or IRS notice that doesn't correspond to anything submitted by the filer.
- Failure to receive expected and routine correspondence from the IRS because the thief has changed the address.

Complete trusted customer questions

The IRS, state tax agency and software providers also share certain data points from returns, including business returns, that help identify a suspicious filing. The IRS and states also are asking that business and tax practitioners provide additional information that will help verify the legitimacy of the tax return.

These "know your customer" procedures are being put in place that include the following questions:

- The name and SSN of the company executive authorized to sign the corporate tax return. Is this person authorized to sign the return?
- Payment history – Were estimated tax payments made? If yes, when were they made, how were they made, and how much was paid?
- Parent company information – Is there a parent company? If yes, who?
- Additional information based on deductions claimed
- Filing history – Has the business filed Form(s) 940, 941 or other business-related tax forms?

Sole proprietorships that file Schedule C and partnerships filing Schedule K-1 with Form 1040 also will be asked to provide additional information items, such as a driver's license number. Providing this information will help the IRS and states identify suspicious business-related returns.

For small businesses looking for a place to start on security, the Federal Trade Commission maintains a Protecting Small Business page which includes a series on cybersecurity and a Cybersecurity for Small Business publication. This is a cooperative effort between the FTC, the National Institute of Standards and Technology, the Department of Homeland Security and the Small Business Administration.

Guard against W-2 scam

All employers – in both the public and private sectors – also are targets for the W-2 scam that has in recent years become one of the more dangerous email scams for tax administration.

These emails appear to be from an executive or organization leader to a payroll or human resources employee. It may start with a simple, "Hey, you in today?" and, by the end of the exchange, all of an organization's Forms W-2 for their employees may be in the hands of cybercriminals. This puts workers at risk for tax-related identity theft.

Because payroll officials believe they are corresponding with an executive, it may take weeks for someone to realize a data theft has occurred. Generally, the criminals are trying to quickly take advantage of their theft, sometimes filing fraudulent tax returns within a day or two.
This scam is such a threat to taxpayers that a special IRS reporting process has been established. Here's an abbreviated list of how to report these schemes:

- Email dataloss@irs.gov to notify the IRS of a W-2 data loss and provide contact information. In the subject line, type "W2 Data Loss" so that the email can be routed properly. Do not attach any employee personally identifiable information data.
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.
- Businesses/payroll service providers should file a complaint with the FBI's Internet Crime Complaint Center (IC3.gov). Businesses/payroll service providers may be asked to file a report with their local law enforcement agency.
- Notify employees so they may take steps to protect themselves from identity theft. The Federal Trade Commission's www.identitytheft.gov provides guidance on general steps employees should take.
- Forward the scam email to phishing@irs.gov.

Employers are urged to put steps and protocols in place for the sharing of sensitive employee information such as Forms W-2. One example would be to have two people review any distribution of sensitive W-2 data or wire transfers. Another example would be to require a verbal confirmation before emailing W-2 data. Employers also are urged to educate their payroll or human resources departments about these scams.

The IRS, state tax agencies and the tax industry are committed to working together to fight against tax-related identity theft and to protect taxpayers. But the Security Summit needs help. People can take steps to protect themselves online.

Taxpayers can visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers, for additional steps to protect themselves and their data from identity theft. Tax professionals can get more information through the Protect Your Clients; Protect Yourself campaign as well as the Tax Security 101 series.

-30-

News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

12 | 07 | 18 DRAFT DRAFT DRAFT DRAFT

IRS, Security Summit Partners warn tax professionals of high risk of data theft attacks

IR-2018-XXX

WASHINGTON – Cybercriminals stepped up their attacks on tax professionals during 2018, prompting the Internal Revenue Service and the Security Summit partners to urge practitioners to take steps to protect client data and their computer networks from these threats.

The IRS also reminded all professional tax preparers that they are required by federal law to create and maintain a written data security plan. Sole practitioners are just as vulnerable to data theft as practitioners in large firms.

The IRS, state tax agencies and the private-sector tax community -- partners in the Security Summit -- are marking National Tax Security Awareness Week with a series of reminders to taxpayers and tax professionals. In the fifth and final part of the special series, the Summit renewed warnings to tax professionals as the 2019 tax season approaches.

IRS Quote

During the 2018 tax filing season, the IRS received five to seven reports per week from tax firms that they have experienced a data theft. Through Nov. 5, 2018, the IRS received xxx reports for the year. That's a xx percent increase from the 182 reports received during the same time in 2017. Generally, these are reports filed by firms, which means hundreds more tax practitioners and tens of thousands of clients are affected.

This increase represents a significant trend in tax-related identity theft, and it's a sign that tax professionals must take stronger measures to safeguard their clients and their business.

Thieves search for client data so they can create a fraudulent tax return that looks legitimate and might bypass IRS filters. They also impersonate tax professionals, using stolen Electronic Filing Identification Numbers (EFINS), Preparer Tax Identification Numbers (PTINs) and Centralized Authorization File (CAF) numbers.

The Gramm-Leach-Bliley Act of 1999 requires all financial institutions, which it also defines as professional tax preparers, to create and maintain information security plans. The Federal Trade Commission, not the IRS, administers this law and created a Safeguards Rule to administer it. Information about the FTC requirements can be found in IRS Publication 4557, Safeguarding Taxpayer Data. The IRS also created a new Publication 5293, Data Security Resources Guide for Tax Professionals, which compiles numerous resources from IRS.gov.
The Security Summit urges tax professionals to seek out cyber experts for assistance with security but at a minimum should take certain safeguards.

Take basic security steps:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open a link or any attachment from a suspicious email. Remember: The IRS never initiates initial contact with a tax pro via email.
- Create a data security plan using IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security – The Fundamentals, by the National Institute of Standards and Technology.
- Review internal controls:
    - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update.
    - Create passwords of at least eight characters; longer is better. Use different passwords for each account, use special and alphanumeric characters, use phrases, password protect wireless devices and consider a password manager program.
    - Encrypt all sensitive files/emails and use strong password protections.
    - Back up sensitive data to a safe and secure external source not connected fulltime to a network.
    - Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
    - Limit access to taxpayer data to individuals who need to know.
    - Check IRS e-Services account weekly for number of returns filed with EFIN.
- Report any data theft or data loss to the appropriate IRS Stakeholder Liaison.
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, Quick Alert, and Social Media.

For 2019 filing season, many tax software vendors will offer two-factor or even three-factor authentication protections for software access. Tax professionals should opt for multi-factor authentication protections whenever it is available. Multi-factor authentication helps prevent cybercriminals from accessing accounts, even if they steal passwords.

Watch for signs of data theft

Tax professionals or their firms may be a victim and not even know it. Here are some common clues to data theft:

- Client e-filed returns begin to reject because returns with their Social Security numbers were already filed;
- Clients who haven't filed tax returns begin to receive authentication letters (5071C, 4883C, 5747C) from the IRS;
- Clients who haven't filed tax returns receive refunds;
- Clients receive tax transcripts that they did not request;
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled or, clients receive an IRS notice that an IRS online account was created in their names;
- The number of returns filed with tax practitioner's Electronic Filing Identification Number (EFIN) exceeds number of clients;
- Tax professionals or clients responding to emails that practitioner did not send;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard;
- Network computers locking out tax practitioners.

Data loss reporting

- Tax professionals who suffer a data theft or loss can assist their clients by immediately reporting the loss to the Internal Revenue Service. The IRS can take steps to either prevent tax-related

identity theft or assist taxpayers to recover faster from tax-related identity theft. More information available at Data Theft Information for Tax Professionals.

- Report client data theft to your local stakeholder liaison. Liaisons will notify IRS Criminal Investigation and others within the agency on your behalf. Speed is critical. If reported quickly, the IRS can take steps to block fraudulent returns in your clients' names and will assist you through the process.

Additional resources:

- Identity Theft Protection: Prevention, Detection and Victim Assistance – See tax pro section.
- Protect Your Clients; Protect Yourself – Awareness campaigns, tips and scam alerts.
- Security Summit – Follow IRS, states and tax industry efforts to combat identity theft.

-30-